On the Resilience Analysis of Interconnected Systems By a Set-Theoretic Approach

Xing Liu, Ionela Prodan, Enrico Zio

On the Resilience Analysis of Interconnected Systems By a Set-Theoretic Approach

X. Liu & I. Prodan
Chair on Systems Science and the Energetic Challenge, European Foundation for New Energy - Electricité de France, École Centrale Paris - Supélec, France.
E. Zio
Chair on Systems Science and the Energetic Challenge, European Foundation for New Energy - Electricité de France, École Centrale Paris - Supélec, France.
Department of Energy, Politecnico di Milano, Italy.

1 INTRODUCTION

In recent years, the protection of critical infrastructure systems (e.g., electric power grids, telecommunication systems, transportation systems and so on) has become an important topic. The notion itself of "critical infrastructure" implies that these interconnected systems are important. They serve our everyday life, e.g. they provide the water and electricity in our homes, for our physical and financial welfare, and support the development of modern societies.

As all systems, these critical infrastructures are exposed to hazardous natural and artificial events, such as earthquake, hurricanes, random failures and sabotages etc., which make them vulnerable (Wolfgang & Zio 2011) Given their importance, the critical infrastructures need very high-levels of reliability and protection (Carlyle et al. 2006, O'Rourke 2007, Murray & Grubesic 2007).

A critical infrastructure is composed of subsystems whose operation is interdependent in different ways and to different degrees (Rinaldi et al. 2001, Rinaldi 2004). The interdependencies and the interactions among the subsystems are the force and the weakness of the critical infrastructures. With respect to the latter, the major risk is that of an initiating failure which propagates from one subsystem to another rendering the global system dysfunctional and unstable. The modeling of this dynamics is quite a challenging task (Buldyrev et al. 2010, Dobson 2008, Pederson et al. 2006).

Several properties make up the capability of a system to provide its function and continue to do so or recover it, in the presence of failures of some of its subsystems. The system must have built-in capacity to resist to the disturbances and be capable to adapt to changing environments. The resilience of a system includes all these properties, specifically, the prevention of and robustness to disturbances, and the capability of recovery from failure.

The analysis and characterization of the resilience of critical infrastructures is receiving a lot of attention from the scientific and technical community. For example, (Nozick et al. 2005) uses a supply-demand graph to represent the interdependency between infrastructures, and Markov and semi-Markov processes for describing the state transitions dynamics. Furthermore, the system performance is measured and analyzed using a probabilistic distribution. Reference (Faraji & Kiyono 2012) proposes a weighted stochastic Petri Net modeling approach for the analysis of critical infrastructures to describe the cascading failure impacts and assess the reliability of the infrastructure. The work in (Bloomfield et al. 2010) builds a stochastic model for the interconnected critical infrastructures, whereby each component is modeled as a random process with a probability to switch between two states, operational and failed. The metric to measure system performance is given in terms of the cascade size resulting from the failure process. A System Dynamics (SD) infrastructure vulnerability assessment framework is proposed in (Tonmoy & El-Zein 2014) to simulate the dependent behaviors of the infrastructure subsystems, and a measure of system performance is provided. An extensible graph-theoretical model is provided in (Svendsen & Wolthusen 2007) for investigating the interdependencies among critical infrastructures. The interactions between their components are modeled through a set of response functions on the graph edges and resources on the nodes. Reference (Reed et al. 2009) introduces a linear input-output model for describing the interdependencies among infrastructures. Methods based on fragility measures and quality functions are proposed to evaluate the system restoration from natural hazards.

Furthermore, (Filippini & Zio 2013, Angelo & Filippini 2013) represent the infrastructure systems in a directed graph and a state dynamics is associated to each subsystem for describing the failure and recovery processes and their interdependent effects. A first attempt of resilience analysis is proposed

based on invariance concepts and asymptotic stability. However, a thorough characterization of the resilience and a metric of the system resilience are not provided.

In the present paper, we embrace a similar approach as in (Angelo & Filippini 2013). We consider a topological model of the infrastructure systems described by a directed graph, with nodes and edges representing the subsystems and the functional dependencies between the subsystems, respectively. Next, we proceed with the modeling of the dynamics of each subsystem and the related interdependencies. For this, we use a state space model with specific dynamics governed by parameters characteristic of the failure and recovery processes. The analysis of the interconnected systems dynamics is performed with the objective of identifying the resilience region for which the system state converges to the operation mode, no matter the disturbances affecting the system. Invariance concepts are used to find the resilience region and to provide conditions on the design parameters, which ensure the successful operation of the interconnected systems. Some interesting behaviors of the system are highlighted, e.g. a chattering behavior.

The rest of the paper is organized as follows. Section 2 introduces the topological description of the interdependent systems, and their associated dynamic model. Section 3 presents the conditions on the design parameters, which ensure the existence of a resilience region. Discussions based on simulation results are presented in Section 4. Finally, Section 5 draws the conclusions and presents the future work.

2 PRELIMINARIES AND PREREQUISITE

This section provides a detailed description of the system modeling and also introduces set invariance notions, which will be instrumental for the resilience analysis of infrastructure systems.

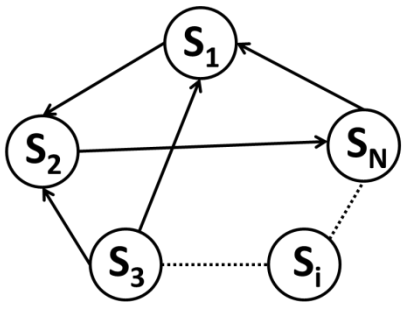

Figure 1. Interconnected system.

2.1 *System modeling*

The entire interconnected system can be represented by a directed graph, with nodes and directed edges describing the network structural characteristics. Figure 1 shows such an interconnected system as a directed graph, where each node represents a subsystem and the direction of the edge connecting two nodes indicates the dependency relationship between two subsystems (i.e., the head node is dependent on the tail node).

Within one interdependent infrastructure system, its subsystems depend on each other by different types of interdependencies. These have different causes and modes of manifestations (Buldyrev et al. 2010, Dobson 2008); formally, these can be described in terms of dynamic models and input/output constraints.

In this paper, we refer in particular to physical interdependencies, cyber interdependencies and also logical interdependencies. In other words, we describe the situation for which one subsystem needs the resources such as power, control signal, water and so on, from another subsystem to keep its functionality. Logical interdependencies can also be taken into account by adding coupling factors to adjust the states of the subsystems depending on their logic configuration. When all the resources needed are provided, the subsystem works in its nominal operation mode; otherwise, it switches into the out-of-operation mode. This is a dynamic behavior common to many interdependent systems and it is well captured by the switching model considered here.

In a switching dynamic model, as the functionality of a subsystem relies on the production or the service provided by other subsystems, the conditions of the switching of this subsystem depend on its input subsystems. From a system-level point of view, a subsystem may continue operating even when the inputs of certain resources are partially unavailable; in this sense, the buffering and restoration processes are both taken into account as two different dynamic modes.

The dynamic model for any subsystem S_i is given by the switching dynamical equations below:

$$\dot{x}_i(t) = \begin{cases} -\mu_i(x_i(t) - \sum_{j\in I_i} \alpha_{ji} x_j(t)) + d_i, & \text{for } x_j \le \sigma_j, \forall j \in I_i \\ \lambda_i\big(1 - x_i(t)\big), & \text{for } x_j \ge \sigma_j, \exists j \in I_i \end{cases} \quad (1)$$

where, I_i is the set of input subsystems of S_i.

Equation (1) represents a switched dynamics in the sense that the value of $\dot{x}_i$ alternates between an operation and a failure mode, depending on the value taken by the current state x_i and the state x_j of all of its input subsystems S_j. Subsystem S_i is in a nominal operation state if all the states of its input subsystems are within their corresponding thresholds σ_j, as described by the first equation in (1). Conversely, if one of its input subsystems fails, the subsystem is in an off-operation state and its dynamical behavior is described by the second equation as a failure process.

Note that for N subsystems we have a total of 2^N modes of functioning for the interconnected system, depending where each of the states x_i resides.

Taking into account the dynamics of the entire system, we can use a switched Linear Time-Invariant (LTI) dynamic equation to describe system behavior:

$$\dot{x}(t) = A_m x(t) + b_m, \quad (2)$$

where, $x(t) = [x_1^T(t), \dots, x_N^T(t)]^T$ represents the state vector of the interconnected system, and matrices $A_m \in \mathrm{R}^{N\times N}$ and $b_m \in R^{N\times 1}$ are constructed accordingly, where $m = 1, \dots, 2^N$.

To describe the interdependencies and the related dynamics of the interconnected infrastructure system, we introduce the following variables and parameters in the system model:

$x_i(t) \in [0,1]$ represents the percentage of the loss of service or the production unrealized by subsystem S_i at time t.

For the subsystem S_i, $x_i(t) = 0$ means that S_i can provide full service, or enough products to meet the requirement, or other resource support, to the other subsystems connected to it as expected/demanded. When the subsystem S_i cannot do so, the value of its state variable augments, $x_i(t) > 0$.

Under the assumption that the actual amount of power produced cannot exceed the intended/demanded service, the value of the state variable is $x_i(t) \in [0,1]$.

The following parameters are introduced to describe the state dynamics:

$\sigma_i \in [0,1]$ indicates the threshold for state variable $x_i(t)$, which allows evaluating if the subsystem S_i can provide the output required for the functioning of its connected subsystems; in other words, it represents the tolerance of system S_i for the percentage of loss of service: if $x_i(t) > \sigma_i$, then the output is insufficient.

$d_i(t) \in [0,1]$ represents both external and internal perturbations, which affect the behavior of the system in nominal operation. It can be instantaneous and more or less strong (e.g. caused by natural disasters, such as earthquake, hurricane or a random fault) or continuous and relatively mild (such as sustained wind, electromagnetic interference, degradation etc.).

In some situations, instantaneous and continuous perturbations can co-exist.

$\lambda_i \in [0,1]$ represents the failure rate for the i^{th} subsystem S_i. The time for the state x_i of S_i to reach the threshold is the time to failure TTF_i, introduced in the following equation:

$$\int_0^{TTF_i} \lambda_i e^{-\lambda_i t} = \sigma_i. \quad (3)$$

From equation (3), we obtain:

$$\lambda_i = -\frac{log(1-\sigma_i)}{TTF_i}. \quad (4)$$

Figure 2 illustrates the variation of the time to failure with the threshold, for a given value of the failure rate. As illustrated, the time to failure increases with the threshold and for larger failure rate values the curve gets closer to the horizontal axis, which means that the subsystem fails earlier at a lower threshold, as reasonable.

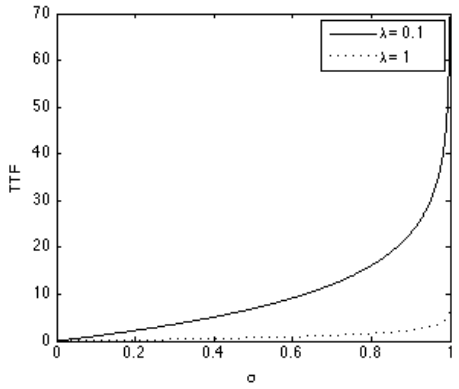

Figure 2. Variation of the time to failure (TTF) as a function of the threshold σ.

$\mu_i \in [0,1]$ represents the recovery rate for subsystem S_i. The time to recovery (TTR_i) is the time that subsystem S_i takes to recover from the failed state to the threshold:

$$\int_0^{TTR_i} \mu_i e^{-\mu_i t} = 1 - \sigma_i. \quad (5)$$

From equation (5), the recovery rate is obtained as:

$$\mu_i = -\frac{log(\sigma_i)}{TTR_i}. \quad (6)$$

The recovery process describes a resilience feature of the system. The time to recovery is a critical characteristic of the resilience of infrastructure systems. In Figure 3, we can see that the time to recovery decreases with the value of the threshold and for large recovery rates the time to recovery is small, as logical.

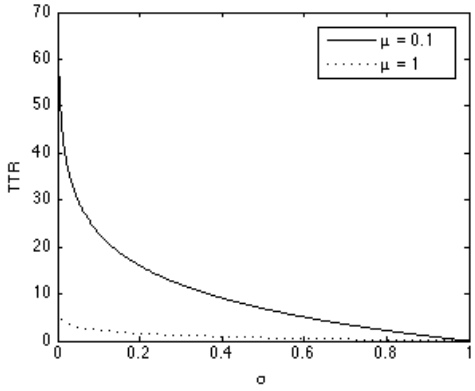

Figure 3. Variation of the time to recovery (TTR) as a function of the threshold σ.

The parameter $\alpha_{ij} \in [0,1]$ is the coupling factor representing the dependency of the subsystem S_i on the subsystem S_j. The term associated to it in the equation (1) represents the rate of the loss of service that the j^{th} subsystem contributes to the i^{th} sub-

system due to the logical dependencies between them.

The dependency relationships among the subsystems represent the logics between producer and user, supplier and consumer, controller and controlled, etc. In these functional relationships, physical quantities and information are produced, consumed or/and transmitted among the subsystems to ensure their functionality. The threshold for one subsystem state is set with respect to all its downstream or output subsystems controlled by it. The value of the threshold indicates the level of tolerance for the downstream subsystems with respect to the acceptable percentage of lost input from the controlling subsystem.

The proposed model not only captures the functional relationship between the subsystems (e.g. due to physical and cyber dependencies) but also takes into account the logical dependency among the subsystems. These are originated from human decisions and actions. The coupling factor allows considering the degree of logical interdependencies in the dynamic process of system evolution.

2.2 *Invariance notions*

In this sub-section, few basic concepts related to the set-theoretic approach are introduced as necessary.

Definition 1 (Equilibrium point). *The point* $x_f \in R^n$ *is an equilibrium point (or fixed point) for the differential equation,*

$$\dot{x}(t) = f(x(t)) \ .$$

If $f(x_f) = 0$.

Definition 2 (Positive invariance). *(Blanchini, 1999) A set* $P \subset R^n$ *is said to be positively invariant for a system of the form*

$$\dot{x}(t) = f(x(t)) \ .$$

If every solution of the equation with initial condition $x(0) \in P$ *verifies* $x(t) \in P$ *for* $t > 0$.

Definition 3 (Robust positive invariance, RPI). *(Blanchini, 1999) A set* $P \subset R^n$ *is said to be robustly positively invariant for a system of the form*

$$\dot{x}(t) = f(x(t), w(t)) \ ,$$

where $w(t) \in W$ *is an exogenous input. If for all* $x(0) \in P$ *and* $w(t) \in W$, *the condition* $x(t) \in P$ *holds for all* $t \geq 0$.

3 DETERMINATION OF THE RESILIENCE REGION

This section presents the necessary conditions on the design parameters for the existence of a resilience region. The region is identified using the invariance concepts introduced in Section 2.2 above.

Proposition 1. *Let there be a convex and compact set* $O \in R^n$ *and consider the dynamics from (2). Whenever equilibrium point* x_f *associated with these dynamics lies into* O, *we have that there exists a subset of O which is an invariant set.*

Proof. If x_f is an equilibrium point for one mode of the switched system

$$\dot{x}(t) = A_m \cdot x(t) + b_m,$$

where $m = 1, \dots, 2^N$.

In any functioning mode of the system, the dynamic equation of each subsystem is an affine equation. Moreover, the eigenvalues λ_A of matrix A satisfy $|\lambda_A| \leq 1$, according to the setting of the parameters. Hence, the system given by (2) is asymptotically stable.

Therefore, $O \in R^N$ is a domain of attraction and we can say that all initial states entering in set O will remain within the set at all future instances, thus O is an invariant set. ■

We assume that x_f is an equilibrium point in a certain dynamic mode of the system, so for the differential equation that describes the system dynamics, the equilibrium point satisfies:

$$0 = A_m \cdot x_f + b_m. \tag{7}$$

In our case, we can compute the equilibrium point for each operation mode:

$$x_f = (I - A_m)^{-1} \cdot b_m. \tag{8}$$

For a system with N subsystems, there are 2^N dynamic modes and the system switches from one to another depending on the states of each subsystem. The state space of the entire system is a hyper-cube $[0,1]^N$, a set divided into 3 main parts: operation region, failure-recovery region and out-of-operation region. In the operation region, all the trajectories of the systems lie in the set $O := [0, \sigma_1] \times [0, \sigma_2] \times \dots \times [0, \sigma_N]$. The out-of-operation region is the opposite, $\bar{O} := [\sigma_1, 1] \times [\sigma_2, 1] \times \dots \times [\sigma_N, 1]$, whereby all the states of all subsystems are of failure and the trajectories converge to an equilibrium point inside this failure region. In the proposed model, the equilibrium points may exist in the operation and out-of-operation regions.

For the operation mode, all the subsystems take the first differential equation:

$$\begin{cases} \dot{x}_1 = -\mu_1\left(x_1 - \sum_{j \in I_1} \alpha_{j1} x_j\right) + d_1 \\ \vdots \\ \dot{x}_i = -\mu_i\left(x_i - \sum_{j \in I_i} \alpha_{ji} x_j\right) + d_i \\ \vdots \\ \dot{x}_N = -\mu_N\left(x_N - \sum_{j \in I_N} \alpha_{jN} x_j\right) + d_N \end{cases}, \tag{9}$$

So the equilibrium point of the operation mode is

$$x_O = (I - A_O)^{-1} \cdot b_O, \tag{10}$$

where, A_O and b_O are matrices with appropriate dimensions.

If the equilibrium point is situated inside the operation region we can say that it is invariant: $x_O \in O$. Thus, one of the conditions on the design parameters for the existence of a resilience region is:

$$[0,\dots,0]^T \leq x_O \leq [\sigma_1,\dots,\sigma_N]^T. \quad (11)$$

For all the initial states in the operation region, the trajectories of system dynamics remain inside the operation region and converge to x_O.

Similarly, the out-of-operation region has the dynamics:

$$\begin{cases} \dot{x}_1 = \lambda_1(1-x_1) \\ \vdots \\ \dot{x}_i = \lambda_i(1-x_i) \\ \vdots \\ \dot{x}_N = \lambda_N(1-x_N) \end{cases}. \quad (12)$$

If there is an equilibrium point,

$$x_{\bar{O}} = (I - A_{\bar{O}})^{-1} \cdot b_{\bar{O}}, \quad (13)$$

it satisfies $x_{\bar{O}} \in \bar{O}$:

$$[\sigma_1,\dots,\sigma_N]^T \leq x_{\bar{O}} \leq [1,\dots,1]^T. \quad (14)$$

Once the state of the system enters the out-of-operation mode, the system cannot recover to the operation region. The next Proposition demonstrates the existence of a resilience region.

Proposition 2. *Let there be a set R_m, which is RPI under the m^{th} functioning mode of dynamics (2). Hence, the resilience region of the interconnected system given in (2) is described by:*

$$R = \bigcup_{m=1}^{2^N} R_m.$$

Proof. In the following, we propose a sketch of the proof. Consider a set R_{ms}, which represents the collection of all the sets where the system initial states reside to O through the corresponding dynamic equation of the m^{th} functioning mode, after s time steps. Therefore, the RPI set under the m^{th} functioning mode can be written as $R_m = \bigcup_{s=1}^{s_{max}} R_{ms}$, where s_{max} is the number of time steps for which the initial states in R_m converge to O. From Proposition 1, we have that O is invariant. This implies that the resilience region of the interconnected system (2) is given by:

$$R = \bigcup_{m=1}^{m=2^N} \bigcup_{s=1}^{s=s_{max}} R_{ms} = \bigcup_{m=1}^{2^N} R_m . \quad \blacksquare$$

We denote the region outside the operation and out-of-operation regions as the failure-recovery region. For initial states inside this region, they may converge either to the operation region or to the out-of-operation region in a finite time. We denote by reachable regions all those regions composed by the system initial states, which converge to the operation region in a finite time. Consequently, the overall resilience region is represented by the union of the operation region and the reachable regions. In other words, the resilience region is defined as the set of all initial states of the system that eventually will reside into the operation region in finite time (i.e. it is composed by the operation region itself plus the reachable regions situated within the failure-recovery region).

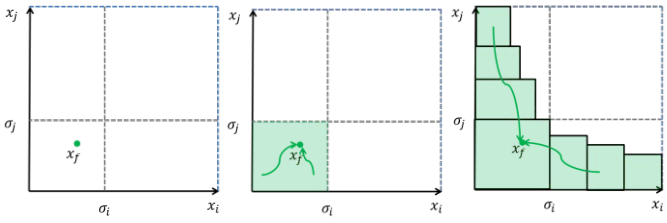

Figure 4. Steps for describing the resilience.

Figure 4 illustrates the steps for describing the resilience region.

Up to this point we can describe the resilience regions as they appear from the interdependencies relationships and the subsystems' characteristics. Indeed, the maximization of the system resilience region is the final design, operation and maintenance goal. We exemplify this by analyzing the response of the system as a function of its parameters, adding an element of control in the dynamics such that a supervisor can actively counteract failure modes and steer the overall system towards the operational functioning region.

4 EXAMPLE AND SIMULATION RESULTS

In this section, we consider a simple example of an interconnected system composed by two subsystems as in Figure 4. Given the methodological flavor of the work, the structure of the system is purposely chosen as simple as possible, in order to not add complexity to the study of the interdependencies among the subsystems and their dynamical behavior, aimed at characterizing the system resilience as a function of the design parameters. The interconnected system in Figure 4 could, for example, represent a system composed by a power supply system and a telecommunication system, whereby the components of the telecommunication system depend on the power supplied by the power supply system which, in turn, for its functioning makes use of the control and monitoring signals provided by the telecommunication system. A theoretical analysis of system resilience is performed and the results are collected into a Table which reports the parameters values of different scenarios of system evolution.

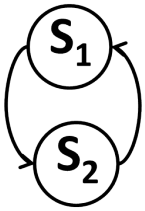

Figure.5. Interconnected system composed by two subsystems.

Consider each subsystem in Figure 5 described by the dynamic equation given in (2). There are four operation modes for the interconnected system, in which the dynamics is represented by the following equations:

Operation mode, where $x(t) \in O \coloneqq [0,\sigma_1]\times[0,\sigma_2]$:

$$\begin{cases}\dot{x}_1(t) = -\mu_1(x_1(t) - \alpha_{21}x_2(t)) + d_1 \\ \dot{x}_2(t) = -\mu_2(x_2(t) - \alpha_{12}x_1(t)) + d_2\end{cases}, \quad (15)$$

Failure-recovery mode 1, where $x(t) \in R_1 \coloneqq [0,\sigma_1]\times[\sigma_2,1]$:

$$\begin{cases}\dot{x}_1(t) = \lambda_1(1 - x_1(t)) \\ \dot{x}_2(t) = -\mu_2(x_2(t) - \alpha_{12}x_1(t))\end{cases}; \quad (16)$$

Failure-recovery mode 2, where $x(t) \in R_2 \coloneqq [\sigma_1,1]\times[0,\sigma_2]$:

$$\begin{cases}\dot{x}_1(t) = -\mu_1(x_1(t) - \alpha_{21}x_2(t)) \\ \dot{x}_2(t) = \lambda_2(1 - x_1(t))\end{cases}; \quad (17)$$

Out-of-operation mode, where $x(t) \in \bar{O} \coloneqq [\sigma_1,1]\times[\sigma_2,1]$:

$$\begin{cases}\dot{x}_1(t) = \lambda_1(1 - x_2(t)) \\ \dot{x}_2(t) = \lambda_2(1 - x_1(t))\end{cases}. \quad (18)$$

Following the procedure described in Section III, the equilibrium states for the operation mode and the out-of-operation mode are identified:

$$x_O = [\frac{\mu_2 d_1 + \alpha_{21}\mu_1 d_2}{(1-\alpha_{12}\alpha_{21})\mu_1\mu_2} \frac{\mu_1 d_2 + \alpha_{12}\mu_2 d_1}{(1-\alpha_{12}\alpha_{21})\mu_1\mu_2}]^T$$

and $x_{\bar{O}} = [1\ 1]^T$.

According to Proposition 1, if x_O is inside the operation region, there exists an invariant set and the equilibrium point locus is the location where all the states in the invariant set will converge. In this case, the invariant set is the operation region itself.

A similar result is found for the out-of operation region, which is also an invariant set with the equilibrium point (1,1) being the attractor in this region.

The conditions for the equilibrium point to be inside the operation region are the following:

$$\begin{cases}0 \le \frac{\mu_2 d_1 + \alpha_{21}\mu_1 d_2}{(1-\alpha_{12}\alpha_{21})\mu_1\mu_2} \le \sigma_1 \\ 0 \le \frac{\mu_1 d_2 + \alpha_{12}\mu_2 d_1}{(1-\alpha_{12}\alpha_{21})\mu_1\mu_2} \le \sigma_2\end{cases}. \quad (19)$$

In order to analyze the intrinsic characteristics of the equilibrium point, we simplify by neglecting the logical interdependencies between the subsystems, i.e., $\alpha_{12} = \alpha_{21} = 0$. In this case, the above conditions become:

$$\begin{cases}0 \le \frac{d_1}{\mu_1} \le \sigma_1 \\ 0 \le \frac{d_2}{\mu_2} \le \sigma_2\end{cases}. \quad (20)$$

Replacing relation (7) in the above equations, we obtain:

$$\begin{cases}TTR_1 \le -\frac{\log(\sigma_1)}{d_1}\sigma_1 \\ TTR_2 \le -\frac{\log(\sigma_2)}{d_2}\sigma_2\end{cases}. \quad (21)$$

This allows highlighting directly the dependence of the time to recovery from the threshold and disturbance values (Figure 6).

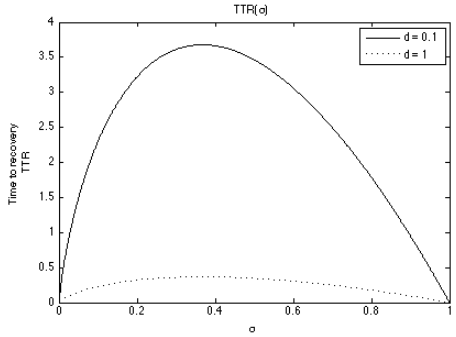

Figure 6. TTR(σ) with fixed disturbance.

If we fix the disturbance d, we can observe the invariance of TTR with the threshold: in the space of parameters (see Figure 5), the time to recovery reaches its maximal value when the threshold is around 0.36.

The next step is the computation of the resilience regions within the two failure-recovery regions, as described in Section III.

Once the states x_1, x_2 enter the out-of-operation region $\bar{O}$ at a certain finite time, the system cannot recover back to the operation region O. But in the two failure-recovery regions R_1 and R_2, it is possible for the system to return to the operation region.

To find the specific resilience region, we compute a resilience curve to separate the end-to-failure and end-to-recovery parts in the failure-recovery region. The situation in R_1 is considered first, whose dynamic equations are (the coupling factors are neglected at first):

$$\begin{cases}\dot{x}_1(t) = \lambda_1(1 - x_1(t)) \\ \dot{x}_2(t) = -\mu_2 x_2(t)\end{cases}. \quad (22)$$

After integration, we obtain:

$$\begin{cases}x_1(t) = 1 + (x_1(0) - 1)e^{-\lambda_1 t} \\ x_2(t) = x_2(0)e^{-\mu_2 t}\end{cases}. \quad (23)$$

From the equations above, we observe that state x_1 tends to diverge to 1 whereas state x_2 converges exponentially to 0. Therefore, there exists a set of states $M \in R_1$ which pass the point (σ_1,σ_2) at a

certain time $t=T$. The set M is represented by the following state equations, with initial conditions $x_1(0)$ and $x_2(0)$:

$$\begin{cases} x_1(T) = 1 + (x_1(0) - 1)e^{-\lambda_1 T} = \sigma_1 \\ x_2(T) = x_2(0)e^{-\mu_2 T} = \sigma_2 \end{cases}. \quad (24)$$

The set of the initial states which pass the point (σ_1, σ_2) at time T is the curve described by:

$$x_1(0) = 1 + (\sigma_1 - 1)\left(\frac{x_2(0)}{\sigma_2}\right)^{\frac{\lambda_1}{\mu_2}}, \quad (25)$$

where $x_1(0) \in [0, \sigma_1]$ and $x_2(0) \in [\sigma_2, 1]$.

In R_2 where the failure is generated in S_1, the set of initial states who pass the point (σ_1, σ_2) can be identified similarly, and we have the curve:

$$x_2(0) = 1 + (\sigma_2 - 1)\left(\frac{x_1(0)}{\sigma_1}\right)^{\frac{\lambda_2}{\mu_1}}, \quad (26)$$

where $x_1(0) \in [\sigma_1, 1]$ and $x_2(0) \in [0, \sigma_2]$.

Figure 7 illustrates the resilience curves, which separate the resilience regions from the non-resilience regions within the failure-recovery region, as described by the equations (25) and (26).

When the design parameters are outside the bounds imposed by conditions (19), the system will not recover i.e., the state trajectories will always converge to the (1,1) equilibrium point outside the (white) operation region as in Figure 8.

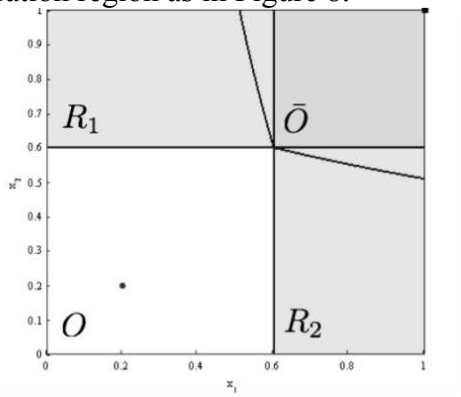

Figure 7. Four operation regions and the curves separating the resilience region and non-resilience region.

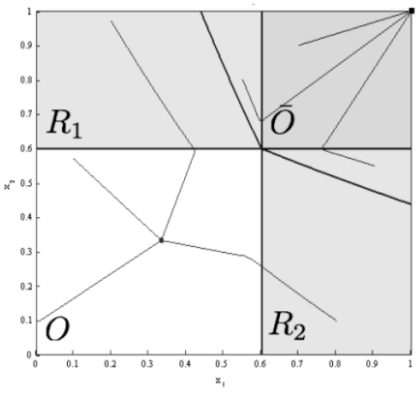

Figure 8. Resilience curve and system trajectories with different initial conditions.

Figure 8 depicts several state trajectories for different initial conditions of the system. We observe that as long as the equilibrium point (denoted as the black dot) is inside the operation region (denoted in white) the system trajectories reside at all times in the resilience region. This means that for the design parameters fulfilling conditions (19) the system will always recover from unexpected event.

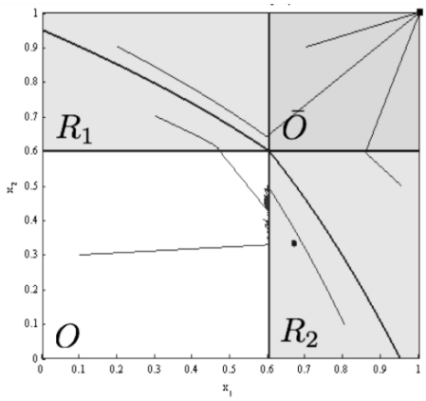

Figure 9. Chattering behavior for the system trajectories with different initial conditions.

The equilibrium point locus is another important aspect for the system resilience. For example, if the equilibrium point of the operation mode resides in the failure-recovery region, we can observe a chattering behavior like the one shown in Figure 9.

Similarly with the previous case, we can determine some conditions on the model parameters such that we can a priori identify the chattering behavior:

In $R_1 := [\sigma_1, 1]\times[0, \sigma_2]$

If the equilibrium point is located in the resilience region of R_1, then:

$$\begin{cases} x_{f_1} = \frac{d_1}{\mu_1} \\ x_{f_2} = \frac{d_2}{\mu_2} \end{cases}. \quad (27)$$

Then, we get the inequalities:

$$\begin{cases} 0 \le \frac{d_1}{\mu_1} \le 1 + (\sigma_1 - 1)\left(\frac{d_2}{\sigma_2 \mu_2}\right)^{\frac{\lambda_1}{\mu_2}} \\ \sigma_2 < \frac{d_2}{\mu_2} \le 1 \end{cases}. \quad (28)$$

In $R_2 := [\sigma_1, 1]\times[0, \sigma_2]$

We get similar results:

$$\begin{cases} \sigma_1 < \frac{d_1}{\mu_1} \le 1 \\ 0 \le \frac{d_2}{\mu_2} \le 1 + (\sigma_2 - 1)\left(\frac{d_1}{\sigma_1 \mu_1}\right)^{\frac{\lambda_2}{\mu_1}} \end{cases}. \quad (29)$$

The conditions (20), (28), (29) allow steering the parameters values in a way to get different scenarios of system evolution, as in Table 1.

The resilience scenario and the chattering scenario are those observed in Figures 7 and 8. To eliminate the chattering behavior, a control law can be added into the model of the interconnected system. Further work will be devoted in the future to the design of control strategies aimed at system chattering behavior elimination.

Parameters	Resilience Scenario	Chattering Scenario 1	Chattering Scenario 2
σ_1	0.6	0.6	0.6
σ_2	0.7	0.7	0.7
d_1	0.3	0.3	0.3
d_2	0.4	0.4	0.4
λ_1	0.1	0.1	0.1
λ_2	0.2	0.2	0.2
μ_1	[0.5,1]	0.7	[0.49,1]
μ_2	[0.57,1]	[0.55,1]	0.8

Table 1. Parameters values.

5 CONCLUSION

This paper adopts a set-theory framework for the resilience analysis of interconnected infrastructure systems. A detailed description of the system dynamics modeling is provided and invariance properties are analyzed to define and identify the resilience region, as a function of the governing parameters. This allows controlling the characteristics of the system resilience properties by design, operation and maintenance properties as represented by the values of the related parameters. An illustration of the analytical power of the framework adopted is provided on an interconnected interconnected system case study, with detailed discussions of its behavior and response to failures and/or disturbances, based on simulation results.

REFERENCES

Angelo, A. & Filippini, R. 2013. "Evaluation of Resilience of Interconnected Systems Based on Stability Analysis." Critical Information Infrastructures Security. Springer Berlin Heidelberg, 180-190.

Bloomfield, R. Buzna, L. Popov, P. Salako, K. & Wright, D. 2010, "Stochastic modelling of the effects of interdependencies between critical infrastructure," in Critical Information Infrastructures Security. Springer, pp. 201–212.

Buldyrev, S. V. Parshani, R. Paul, G. Stanley, H. E. & Havlin, S. 2010. "Catastrophic cascade of failures in interdependent networks," Nature, vol. 464, no. 7291, pp. 1025–1028.

Carlyle, G. Salmeron, M. J. & Wood, K. 2006. "Defending critical infrastructure," Interfaces, vol. 36, no. 6, pp. 530–544.

Dobson, I. 2008. "Analysis of cascading infrastructure failures," Wiley Hand-book of Science and Technology for Homeland Security.

Faraji, M. & Kiyono, J. 2012. "Infrastructure performance oriented reliability using assessment using weighed stochastic petri net," 15WCEE, Lisboa.

Filippini, R. & Zio, E. 2013. "integrated resilience and risk analysis framework for critical infrastructures", in Proceeding of ESREL conference, pp. 2001-2008.

Murray, A. T. & Grubesic, T. H. 2007. Critical infrastructure: reliability and vulnerability. Springer Berlin, vol. 16.

Nozick, L. K. Turnquist, M. A. Jones, D. A. & Davis, J. R. 2005. "Assessing the performance of interdependent infrastructures and optimising investments," International journal of critical infrastructures, vol. 1, no. 2, pp.144–154.

O'Rourke, T. D. 2007. "Critical infrastructure, interdependencies, and resilience," Bridge-Washington-National Academy of Engineering, vol. 37, no. 1, p. 22.

Pederson, P. Dudenhoeffer, D. Hartley, S. & Permann, M. 2006. "Critical infrastructure interdependency modeling: a survey of us and international research," Idaho National Laboratory, pp. 1–20.

Reed, D. A. Kapur, K. C. & Christie, R. D. 2009. "Methodology for assessing the resilience of networked infrastructure," Systems Journal, IEEE, vol. 3, no. 2, pp. 174–180.

Rinaldi, S. M. Peerenboom, J. P. & Kelly, T. K. 2001. "Identifying, un-derstanding, and analyzing critical infrastructure interdependencies," Control Systems, IEEE, vol. 21, no. 6, pp. 11–25.

Rinaldi, S. M. 2004. "Modeling and simulating critical infrastructures and their interdependencies," in System sciences, 2004. Proceedings of the 37th annual Hawaii international conference on. IEEE, pp. 54–61.

Svendsen, N. K. & Wolthusen, S. D. 2007. "Connectivity models of inter-dependency in mixed-type critical infrastructure networks,"Information Security Technical Report, vol. 12, no. 1, pp. 44–55.

Tonmoy, F. & El-Zein, A. 2014. "Vulnerability of infrastructure to sea level rise: A combined outranking and system-dynamics approach," in Safety, Reliability and Risk Analysis: Beyond the Horizon. CRC Press.

Wolfgang, K. & Zio, E. 2011. Vulnerable systems. Springer.